CLAIMS

1. (Currently Amended) A computer-implemented method, comprising:

on a device configured as part of a security infrastructure to receive messages, receiving a message;

selecting a first set of security information from a first plurality of sets of security information as a function of a property of the message, wherein the first set of security information comprises security settings;

selecting a second set of security information from a second plurality of sets of security information as a function of the first set, wherein the second set of security information comprises security settings and wherein the second set is a distinct set from that of the first set; and

applying the second set of security information to the message.

2. (Original) The method of claim 1, wherein applying the second set of security information to the message further comprises applying security information derived from the first set.

3. (Original) The method of claim 1, further comprising determining whether the message satisfies a security requirement derived from security information of the second set.

4. (Original) The method of claim 3, wherein determining whether the message satisfies a security requirement derived from security information of the second set further comprises determining whether the message satisfies a security requirement derived from security information of the first set.

5. (Original) The method of claim 3, further comprising rejecting the message if the message does not satisfy the security requirement.

6. (Original) The method of claim 5, further comprising accepting the message if the message satisfies all security requirements included in the second set.

7. (Original) The method of claim 6, wherein the message is received after transmission from a sender.

8. (Original) The method of claim 1, wherein the message is to be transmitted to another process.

9. (Previously Presented) The method of claim 8, further comprising securing the message before the message is transmitted.

10. (Original) The method of claim 1, wherein the second plurality of sets of security information are shared between nodes of a network.

11. (Original) The method of claim 1, wherein the first set is selected using an XPath-based expression to match a preselected pattern.

12. (Original) The method of claim 1, wherein the first set is selected using Simple Object Access Protocol (SOAP) actions.

13. (Previously Presented) A machine-readable storage medium having instructions for performing the method of claim 1.

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Previously Presented) A system comprising:

a processor;

a memory coupled to the processor to store at least a portion of a plurality of datastores;

a first datastore to include a first plurality of sets of security settings related to an application residing in the system, wherein the first plurality of sets define messages that must be secured;

a second datastore to include a second plurality of sets of security settings, wherein the second plurality of sets specify settings and operations for securing messages, and wherein a set of the first plurality of sets is associated with a set of the second plurality of sets; and

a module to select the first set from the first plurality of sets as a function of a property of a received message.

20. (Original) The system of claim 19 wherein the first and second datastores are part of a single larger datastore.

21. (Original) The system of claim 19 wherein the module is further to apply security information included in a second set of the second plurality of sets to the received message.

22. (Original) The system of claim 21, wherein the module is further to apply security information included in the first set to the received message.

23. (Previously Presented) The system of claim 21, wherein the module is further to determine whether the received message satisfies a security requirement included in security information of the second set.

24. (Original) The system of claim 23, wherein the module is further to reject the message if the message does not satisfy the security requirement.

25. (Original) The system of claim 24, wherein the module is further to accept the message if the message satisfies all security requirements included in the security information of the second set.

26. (Original) The system of claim 19, further comprising a third datastore to include mappings from sets of the first plurality of sets to sets of the second plurality of sets, wherein the second set is associated with the first set by a mapping included in the third datastore.

27. (Original) The system of claim 19, wherein the module is to select the first set using an XPath-based expression to match a preselected pattern.

28. (Original) The system of claim 19, wherein the module is to select the first set using a predetermined Simple Object Access Protocol (SOAP) action.

29. (Original) The system of claim 19, wherein the second plurality of sets are shared between nodes of the system.

30. (Canceled)

31. (Previously Presented) A machine-readable storage medium having instructions for performing a method, comprising:

steps for receiving a message;

steps for selecting a first set of security information from a first plurality of sets of security information as a function of a property of the message, wherein the first set of security information comprises security settings that define types of messages that must be secured and wherein the types of messages that must be secured are defined and provided by an application developer;

steps for selecting a second set of security information from a second plurality of sets of security information as a function of the first set, wherein the second set of security information comprises security settings that specify particular operations and settings for securing the messages, wherein the particular operations and settings comprise algorithms to be used in signing and encrypting the messages; and

steps for applying the second set of security information to the message.

32. (Previously Presented) The machine-readable storage medium of claim 31, further comprising steps for determining whether the message satisfies a security requirement derived from the first and/or second sets.

33. (Previously Presented) The machine-readable storage medium of claim 32, further comprising steps for rejecting the message if the message does not satisfy the security requirement.

34. (Previously Presented) The machine-readable storage medium of claim 32, further comprising steps for accepting the message if the message satisfies all security requirements derived from the first and second sets.

35. (Previously Presented) The machine-readable storage medium of claim 34, wherein the message is received after transmission from a sender.

36. (Previously Presented) The machine-readable storage medium of claim 31, wherein the message is to be transmitted to another process.

37. (Previously Presented) The machine-readable storage medium of claim 36, further comprising steps for securing the message before the message is transmitted.

38. (Previously Presented) The machine-readable storage medium of claim 31, wherein the second plurality of sets of security information are shared between nodes of a network.

39. (Previously Presented) The machine-readable storage medium of claim 31, wherein the steps for selecting the first set uses an XPath-based expression to match a preselected pattern.

40. (Previously Presented) The machine-readable storage medium of claim 31, wherein the steps for selecting the first set selects the first set using Simple Object Access Protocol (SOAP) actions.